2/5/1
DIALOG(R)File 351:Derwent WPI

012628490 **Image available**
WPI Acc No: 1999-434594/ **199937**
XRPX Acc No: N99-323923

Document existence certification method in computer network - involves transmitting hash URL to registrant terminal, after acquiring document using server

Patent Assignee: HITACHI LTD (HITA)
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
JP 11175512	A	19990702	JP 97338364	A	19971209	199937	B

Priority Applications (No Type Date): JP 97338364 A 19971209
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
JP 11175512	A		11	G06F-017/21	

Abstract (Basic): JP 11175512 A

NOVELTY - A server (1) acquires a document (11) using designated URL, after receiving registration demand of existence proof information from registrant terminal (3). A hash (14) is generated from registration date, document URL and the document and their link is registered in a database (13). The hash URL is then transmitted to registrant terminal.

USE - For document existence certification in client server network.

ADVANTAGE - Duplication object of document can be preserved locally and reliability of truth or falsehood can be given to other perusal person. DESCRIPTION OF DRAWING(S) - The figure shows systematic diagram of certification system. (1) Server; (3) Registrant terminal; (11) Document; (13) Database; (14) Hash.

Dwg.1/12

Title Terms: DOCUMENT; EXIST; CERTIFY; METHOD; COMPUTER; NETWORK; TRANSMIT; HASH; TERMINAL; AFTER; ACQUIRE; DOCUMENT; SERVE
Derwent Class: P85; T01
International Patent Class (Main): G06F-017/21
International Patent Class (Additional): G06F-015/00; G09C-001/00
File Segment: EPI; EngPI

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号

特開平11－175512

(43)公開日　平成11年(1999)７月２日

(51)Int.Cl.[6]		識別記号	FI		
Ｇ０６Ｆ	17/21		Ｇ０６Ｆ	15/20	５９０Ｚ
	15/00	３１０		15/00	３１０Ａ
// Ｇ０９Ｃ	1/00	６４０	Ｇ０９Ｃ	1/00	６４０Ｚ
			Ｇ０６Ｆ	15/20	５７０Ｒ

審査請求　未請求　請求項の数３　ＯＬ　（全 11 頁）

(21)出願番号　特願平9－338364

(22)出願日　平成９年(1997)12月９日

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地

(72)発明者　森田　光
神奈川県横浜市都筑区加賀原二丁目２番
株式会社日立製作所ビジネスシステム開発センタ内

(72)発明者　千葉　寛之
神奈川県横浜市都筑区加賀原二丁目２番
株式会社日立製作所ビジネスシステム開発センタ内

(74)代理人　弁理士　高橋　明夫　（外１名）

最終頁に続く

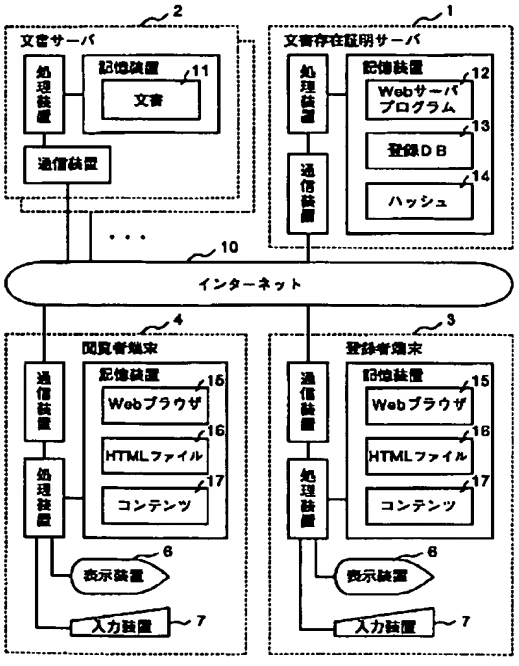
(54)【発明の名称】　文書の存在証明に関するプログラム

(57)【要約】

【課題】　オリジナル文書が特定の日付に特定の格納場所に存在したことを証明する。

【解決手段】　登録者端末３は、文書１１の複製物をコンテンツ１７として保存する。登録者端末３からの存在証明情報の登録要求に応答して文書存在証明サーバ１は、指定されたＵＲＬによって文書１１を取得し、登録日付、文書ＵＲＬ及び文書１１の内容からハッシュ１４を生成し、そのリンクを登録ＤＢ１３に登録し、登録者端末３へハッシュＵＲＬを通知する。登録者端末３はハッシュＵＲＬを含む存在確認ページを作成してＨＴＭＬファイル１６に保存する。コンテンツ１７及びＨＴＭＬファイル１６の複製物を取得した閲覧者端末４は、コンテンツ及び存在確認ページ中の登録日付、文書ＵＲＬに基づいてハッシュを生成し、文書存在証明サーバ１から取得したハッシュ１４と比較してオリジナル文書の存在を検証する。

図　1



【特許請求の範囲】

【請求項１】コンピュータ読み取り可能な記憶媒体に実体化されたコンピュータプログラムであり、特定の文書が特定の日付に特定の格納場所に存在したことを証明するクライアント計算機の支援をするサーバ計算機によって実行されるプログラムであって、該プログラムは下記のステップを含む：

（ａ）クライアント計算機からの文書の存在証明情報の登録要求に応答して指定された文書の格納場所から該文書のオリジナルを取得し、（ｂ）該文書のコンテンツ、該文書の格納場所及び登録日付を含む情報から縮小された代替情報を生成し、（ｃ）該代替情報を記憶装置に保存し、（ｄ）クライアント計算機が該代替情報に基づいて該文書の存在証明を実施可能なようにクライアント計算機へ該代替情報の格納場所を通知する。

【請求項２】コンピュータ読み取り可能な記憶媒体に実体化されたコンピュータプログラムであり、特定の文書が特定の日付に特定の格納場所に存在したことを証明するクライアント計算機と該文書のオリジナルのコンテンツ、該文書の格納場所及び登録日付を含む情報から生成された縮小された代替情報を登録するサーバ計算機とを有するシステムのうち、該クライアント計算機によって実行されるプログラムであって、該プログラムは下記のステップを含む：

（ａ）該文書の複製物のコンテンツ、該文書の格納場所及び登録日付から縮小された代替情報を生成し、（ｂ）該サーバ計算機から取得した対応する代替情報と生成した代替情報とが一致することによって該文書の存在証明をする。

【請求項３】該プログラムは、さらに上記（ａ）及び（ｂ）のステップの前に、該サーバ計算機へ該文書の格納場所を送信して該代替情報の登録要求を行い、該代替情報の格納場所を受信するステップを含むことを特徴とする請求項２記載のコンピュータプログラム。

【発明の詳細な説明】

【０００１】

【本発明の属する技術分野】本発明は、ネットワーク上に存在する文書が特定の日付に特定の格納場所に存在したことを証明する技術に係わり、特に文書の存在証明を支援するサーバ計算機に登録された存在証明情報を利用して文書の存在証明を行う方法に関する。

【０００２】

【従来の技術】Ｗｏｒｌｄ　Ｗｉｄｅ　Ｗｅｂを用いることによって、ネットワーク上に分散したサーバが格納する文書をＷｅｂページの形式で不特定多数のクライアントに公開し、さらに他の文書の参照を行うために他の文書の格納場所を示すリンクを文書中に埋め込むことによってクライアントはネットワーク上に分散する数多くの文書を効率良く閲覧することが可能となる。

【０００３】しかし各サーバの管理者もしくは各文書の提供者が異なるため、文書によってはリンク先のＷｅｂページなどの文書が変更されたり消滅する可能性がある。そのためその文書の改変もしくは消滅などといった事態を回避する手段の一つとして、各個人が個別に特定の文書の複製物を保存することが挙げられる。この場合、このようにして保存された文書のオリジナルが元々のリンク先によって示される格納場所にローカルに保存された通りの内容で存在したものか否かを証明する手段は存在しない。

【０００４】

【発明が解決しようとする課題】以上述べたように、リンク先のＷｅｂページなどの文書の変更や消滅などに対処するためには、その文書を利用しようとする者が個別に保存することが考えられるが、そのようにして保存された文書のオリジナルが元々の格納場所によって同定される場所に存在したものか否かを証明する手段は存在せず、この文書の複製物を個別に保存した者がこの複製物を他者に提供する際に、この文書のオリジナルの発信源を証明することができないという問題があった。

【０００５】本発明は上記事情に鑑みてなされたものであり、その目的とするところは、特定の文書が特定の日付に特定の格納場所に存在したことを示す存在証明情報を登録する手段を提供することにあり、またこの存在証明情報を利用して文書の存在証明をする手段を提供することにある。

【０００６】

【課題を解決するための手段】本発明に関する情報システムは、文書の存在証明情報の登録を要求する登録者のクライアント計算機、この登録要求に応答して文書の存在証明情報を登録するサーバ計算機及び文書の複製物の提供を受け元々の文書の存在証明をする閲覧者のクライアント計算機を有する。サーバ計算機で実行されるプログラムは、クライアント計算機からの文書の存在証明情報の登録要求に応答して指定された文書の格納場所からこの文書のオリジナルを取得し、文書のコンテンツ、文書の格納場所及び登録日付を含む情報から縮小された代替情報を生成し、この代替情報を記憶装置に保存し、クライアント計算機がこの代替情報に基づいてオリジナル文書の存在証明を実施可能なようにクライアント計算機へ代替情報の格納場所を通知する。また閲覧者のクライアント計算機で実行されるプログラムは、文書の複製物のコンテンツ、文書の格納場所及び登録日付から縮小された代替情報を生成し、サーバ計算機から取得した対応する代替情報と生成した代替情報とが一致するのを確認することによってオリジナル文書の存在証明をする。

【０００７】本発明によれば、登録日付以後にオリジナル文書が改変されたか消滅したかに関わらず元々の文書の存在を証明することができる。

【０００８】

【発明の実施の形態】以下本発明の一実施形態について

図面を用いて詳細に説明する。

【０００９】図１は、Ｗｏｒｌｄ　Ｗｉｄｅ　Ｗｅｂに関するシステム構成を示す構成図である。文書サーバ２は処理装置、記憶装置及びインターネット１０に接続するための通信装置を含む計算機であり、その記憶装置には元々の提供者から提供された文書１１のオリジナルを格納する。文書存在証明サーバ１は、公に認められた第３者機関のサーバであり、同様に処理装置、記憶装置及び通信装置を含む計算機であり、その記憶装置にはＷｅｂサーバプログラム１２、登録データベース（ＤＢ）１３及びハッシュ１４を格納する。ハッシュ１４は文書１１のコンテンツ等から計算されるハッシュである。登録ＤＢ１３は、文書１１の存在証明情報の一部を格納する。この存在証明情報は、登録日付、文書１１のＵｎｉｆｏｒｍＲｅｓｏｕｒｃｅ　Ｌｏｃａｔｏｒ（以下ＵＲＬと略す）、ハッシュ１４のＵＲＬ等を含む。Ｗｅｂサーバプログラム１２は、従来のＷｅｂサーバプログラムの機能のほかに登録者端末３からの要求に従って文書１１のコンテンツ等からハッシュ１４を計算して記憶装置に格納するとともに存在証明情報を登録ＤＢ１３に格納する。

【００１０】登録者端末３は、処理装置、記憶装置、通信装置、表示装置６及び入力装置７を含むパソコンのようなクライアント計算機であり、その記憶装置にはＷｅｂブラウザ１５、ＨＴＭＬ（Ｈｙｐｅｒｔｅｘｔ　Ｍａｒｋｕｐ　Ｌａｎｇｕａｇｅ）ファイル１６及びコンテンツ１７を格納する。コンテンツ１７は文書１１の複製物としてローカルに保存されるものである。ＨＴＭＬファイル１６は文書１１の存在確認をするための表示ページを格納するファイルである。Ｗｅｂブラウザ１５は、従来のＷｅｂブラウザの機能のほかに文書存在証明サーバ１に文書１１についての存在証明情報の登録を要求し、文書存在証明サーバ１に存在証明情報が登録されたとき文書１１の存在確認をするための存在確認ページを生成してＨＴＭＬファイル１６に格納するプログラムである。表示装置６はコンテンツ１７、ＨＴＭＬファイル１６等を表示する装置であり、入力装置７はＷｅｂブラウザ１５に対して登録等の指示をするキーボード、マウス等の入力装置である。

【００１１】閲覧者端末４は、処理装置、記憶装置、通信装置、表示装置６及び入力装置７を含むパソコンのようなクライアント計算機であり、その記憶装置にはＷｅｂブラウザ１５、ＨＴＭＬファイル１６及びコンテンツ１７を格納する。コンテンツ１７は登録者端末３のコンテンツ１７の複製物として保存されるものである。ＨＴＭＬファイル１６は登録者端末３のＨＴＭＬファイル１６の複製物として保存されるものである。Ｗｅｂブラウザ１５は、従来のＷｅｂブラウザの機能のほかにコンテンツ１７等からハッシュを計算し、ＨＴＭＬファイル１６中のハッシュＵＲＬに基づいて文書存在証明サーバ１にアクセスしてハッシュ１４を取得し、両ハッシュの一致を確認する検証処理を行うプログラムである。表示装置６はコンテンツ１７、ＨＴＭＬファイル１６等を表示する装置であり、入力装置７はＷｅｂブラウザ１５に対して検証等の指示をするキーボード、マウス等の入力装置である。

【００１２】登録者端末３は、入力装置７からの指示に従って文書サーバ２にアクセスし、文書１１の複製物を取得し、コンテンツ１７として記憶装置に格納し、表示装置６上に表示する。入力装置７を介してこのコンテンツ１７の存在証明情報の登録を要求されたとき、Ｗｅｂブラウザ１５は、文書１１のＵＲＬを文書存在証明サーバ１へ送信して登録要求を行う。文書存在証明サーバ１のＷｅｂサーバプログラム１２はこの要求を受け取り、文書サーバ２にアクセスして文書１１を取得し、登録日付、文書ＵＲＬ及び文書１１のコンテンツからハッシュ１４を計算して記憶装置に格納し、登録日付、文書ＵＲＬ及びハッシュＵＲＬを含む存在証明情報を作成して登録ＤＢ１３に格納する。また登録者端末３にはハッシュＵＲＬを返送する。登録者端末３のＷｅｂブラウザ１５は、登録日付、文書ＵＲＬ、コンテンツ１７へのリンク及び受け取ったハッシュＵＲＬから成る存在確認ページを生成し、存在確認を検証してから存在確認ページをＨＴＭＬファイル１６に格納する。閲覧者端末４のＷｅｂブラウザ１５は、登録者端末３からコンテンツ１７及びＨＴＭＬファイル１６の複製物を取得してその記憶装置に格納する。入力装置７を介してコンテンツ１７の存在確認の検証を要求されたとき、Ｗｅｂブラウザ１５は、コンテンツ１７、ＨＴＭＬファイル１６中の登録日付及び文書ＵＲＬからハッシュを計算し、ＨＴＭＬファイル１６中のハッシュＵＲＬに基づいて文書存在証明サーバ１にアクセスしてハッシュ１４を取得して両ハッシュが一致することを確認する検証処理を行う。

【００１３】図２は、登録ＤＢ１３のデータ構成を示す図である。登録ＤＢ１３の各レコードは、登録日付、メールアドレス、文書ＵＲＬ及びハッシュＵＲＬから構成される。登録日付は本レコードの登録を行った日付、メールアドレスは登録者の電子メールアドレス、文書ＵＲＬは存在証明する文書１１の元の存在場所を示すＵＲＬ、ハッシュＵＲＬはこの文書に関するハッシュ１４を格納する文書存在証明サーバ１の格納場所を示すＵＲＬである。各レコードに登録者のメールアドレスを加える理由は、同一日に同一文書ＵＲＬについて複数の登録者から登録要求があった場合に各登録者ごとのレコードを特定するためである。従ってメールアドレスの代わりにユーザＩＤなど登録者を識別する他の識別子を用いてもよい。

【００１４】図３は、ＨＴＭＬファイル１６の内容を示す図である。ＨＴＭＬファイル１６は、ＨＴＭＬで記述され、存在確認ページを表示するために使用され、登録

日付、コンテンツ１７の元の存在場所を示すＵＲＬ、当該登録者端末３が保有するコンテンツ１７の格納場所（リンク）及び文書存在証明サーバ１に保存されたハッシュのＵＲＬを含む。コンテンツ１７のリンクとは、登録者端末３のＵＲＬに特定のコンテンツ１７の識別子を付加したものである。ハッシュのＵＲＬとは、文書存在証明サーバ１のＵＲＬに特定のハッシュの識別子を付加したものである。

【００１５】図４は、登録者端末３のＷｅｂブラウザ１５の処理の流れを示すフローチャートであり、特にハッシュを含む文書の存在証明情報を文書存在証明サーバ１に登録する処理の手順を示す。Ｗｅｂブラウザ１５は、コンテンツ１７を表示装置６上に表示し、入力装置７からコンテンツ１７の存在証明情報の登録を指示されたとき、文書の元の存在場所を示すＵＲＬに電子署名を施した後、この電子署名を施した文書ＵＲＬと登録者の電子メールアドレスを文書存在証明サーバ１へ送信し、登録要求を行う（ステップ２１）。ここで電子署名を施すとは、ＲＳＡ研究所の提唱するＰＫＣＳ（Ｐｕｂｌｉｃ－Ｋｅｙ　Ｃｒｙｐｔｏｇｒａｐｈｙ　Ｓｔａｎｄａｒｄｓ）＃７で定義される手法を用いて対象データに署名を施すことである。次に後で利用できるように当日の日付(グリニッジ標準時)、文書ＵＲＬ及び文書のコンテンツを登録者端末３の記憶装置に格納する（ステップ２２）。文書存在証明サーバ１から登録情報を受信したとき（ステップ２３）、その登録結果を調べて登録が行われたか否かを判定する（ステップ２４）。登録が行われなかった場合（ステップ２４Ｎｏ）、ステップ２１に戻る。登録が行われた場合（ステップ２４Ｙｅｓ）、記憶装置に格納された登録日付、文書ＵＲＬ及びステップ２３で受信したハッシュＵＲＬを表示装置６に表示し、次いでこれにコンテンツ１７へのリンクを加えた存在確認ページを生成して表示装置６に表示する（ステップ２５）。入力装置７を介して検証が指示されたとき、記憶装置に格納した文書ＵＲＬ、コンテンツ及び登録日付をタプルとしてハッシュを計算する（ステップ２６）。ここでハッシュの計算とは、例えば１６０ビットＳＨＡ－１ハッシュを求めること、すなわちＨをハッシュ関数、ｔをタプルとするとＨ（ｔ）を求めることである。ハッシュは文書ＵＲＬ、登録日付及び元の文書１１の縮小された代替情報とみなせる。次にステップ２３で登録情報として受信したハッシュＵＲＬにアクセスし、文書存在証明サーバ１に保存されたハッシュ１４を取得する（ステップ２７）。次に取得したハッシュに文書存在証明サーバ１の電子署名が施されているか否か判定し、かつ取得したハッシュとステップ２６で計算したハッシュとを比較して両者が一致するか否か判定する（ステップ２８）。ハッシュの電子署名とは、ハッシュが文書存在証明サーバ１の秘密鍵によって暗号化されたものであり、この暗号化されたハッシュを登録者端末３のもつ公開鍵によって復号することによって文書存在証明サーバ１が認めたハッシュか否かを判定可能である。文書存在証明サーバ１の署名がないか両ハッシュが一致しない場合には（ステップ２８Ｎｏ）、処理を中止する。文書存在証明サーバ１の署名があり両ハッシュが一致した場合には（ステップ２８Ｙｅｓ）、生成した存在確認ページをＨＴＭＬファイル１６として記憶装置に格納する（ステップ２９）。ステップ２５～２８は、文書の存在証明情報が正しく文書存在証明サーバ１に登録されたことを検証する処理である。なおすでに文書存在証明サーバ１に登録された文書の存在証明情報を削除する場合には、登録日付、文書ＵＲＬ及びメールアドレスを文書存在証明サーバ１に送信し、削除要求を行えばよい。

【００１６】図５は、文書存在証明サーバ１のＷｅｂサーバプログラム１２の処理のうち、文書の存在証明情報を登録する処理の流れを示すフローチャートである。登録者端末３から登録要求又は削除要求を受信すると（ステップ３１）、受信した文書ＵＲＬに署名が施されているか否かを判定する（ステップ３２）。署名が確認できない場合（ステップ３２Ｎｏ）、記憶装置上の処理情報として登録結果（Ｒｅｓｕｌｔ）に未登録、エラーコード（ｅｒｒｏｒＣｏｄｅ）に不正署名（ｉｎｖａｌｉｄ　Ｓｉｇｎａｔｕｒｅ）をセットし（ステップ３３）、ステップ４６へ行く。署名が施されている場合（ステップ３２Ｙｅｓ）、要求が削除要求か否か判定する（ステップ３４）。削除要求であれば（ステップ３４Ｙｅｓ）、後述の削除処理を行う（ステップ３５）。登録要求であれば（ステップ３４Ｎｏ）、文書１１のコンテンツを取得するために受信した文書ＵＲＬが指す文書サーバ２にアクセスする（ステップ３６）。次に文書ＵＲＬにアクセスできたか否かを判定する（ステップ３７）。アクセスできなかった場合（ステップ３７Ｙｅｓ）、記憶装置上のカウンタに１を加え（ステップ３８）、カウンタの内容が所定値以下か否かを判定する（ステップ３９）。所定値以下であれば（ステップ３９Ｙｅｓ）ステップ３６に戻って文書ＵＲＬへのアクセスを再試行する。カウンタの内容が所定値を越えたとき（ステップ３９Ｎｏ）、処理情報の登録結果に未登録、エラーコードに取得不能（Ｕｎｒｅａｃｈａｂｌｅ）をセットし（ステップ４０）、ステップ４６へ行く。文書サーバ２から文書１１のコンテンツを取得したとき（ステップ３７Ｎｏ）、取得したコンテンツを検索してこの文書を文書存在証明サーバ１に登録することに関して文書の提供者が同意する旨の署名があるか否かを判定する（ステップ４１）。同意の署名がない場合には（ステップ４１Ｎｏ）、処理情報の登録結果に未登録、エラーコードに提供者拒否（ＡｕｔｈｏｒＲｅｊｅｃｔ）をセットし（ステップ４２）、ステップ４６へ行く。同意の署名がある場合には（ステップ４１Ｙｅｓ）、文書ＵＲＬ、取得したコンテンツ及び登録当日の日付からハッシュを計算

し、ハッシュに署名を施し（ステップ４３）、署名とハッシュを記憶装置上のハッシュ１４に格納し、登録ＤＢ１３に登録レコードを追加する（ステップ４４）。ハッシュの計算方式は、ステップ２６の計算方式と同じである。登録する情報は、登録者端末３から受信したメールアドレス、文書ＵＲＬと、登録日付、ハッシュ１４の格納場所を示すハッシュＵＲＬである。次に処理情報の登録結果に登録済（ＯＫ）をセットし、ハッシュＵＲＬを付加する（ステップ４５）。最後に登録情報として登録結果（登録済）とハッシュＵＲＬ又は登録結果（未登録）とエラーコードを登録者端末３へ送信する（ステップ４６）。なおＷｅｂサーバプログラム１２は、登録者端末３又は閲覧者端末４からハッシュＵＲＬを指定したハッシュの要求があったとき、指定された格納場所からハッシュ１４を取り出して送信する。

【００１７】図６は、Ｗｅｂサーバプログラム１２の処理のうち、文書の存在証明情報を削除する処理の流れを示すフローチャートである。Ｗｅｂサーバプログラム１２は、登録者端末３から受信した登録日付、文書ＵＲＬおよびメールアドレスをキーとして登録ＤＢ１３を検索し（ステップ５１）、該当するレコードが存在するか否かを判定する（ステップ５２）。該当データが存在する場合には（ステップ５２Ｙｅｓ）、該当するレコードのハッシュＵＲＬの指すハッシュ１４及び登録ＤＢ１３上の該当レコードを削除する（ステップ５３）。次に記憶装置上の処理情報として削除結果に削除済（ＯＫ）をセットし（ステップ５４）、削除結果を登録者端末３へ通知する（ステップ５５）。該当データが存在しない場合には（ステップ５２Ｎｏ）、処理情報の削除結果に未削除、エラーコードに「データが見当らない」（ＤａｔａＮｏｔＦｏｕｎｄ）をセットし（ステップ５６）、ステップ５５へ行く。ステップ５５では削除結果とエラーコードを登録者端末３へ通知する。

【００１８】文書の閲覧者によって操作される閲覧者端末４のＷｅｂブラウザ１５は、登録者端末３からコンテンツ１７を取得し、閲覧者端末４の記憶装置に格納し、表示装置６上に表示することが可能であり、閲覧者による文書の閲覧が可能である。以下閲覧者の必要性によってこの文書が元の存在場所に存在したことを検証するときの閲覧者端末４の検証処理について説明する。

【００１９】図７は、閲覧者端末４のＷｅｂブラウザ１５による検証処理の流れを示すフローチャートである。入力装置７からの指示に従ってＷｅｂブラウザ１５は、登録者端末３にアクセスし存在確認ページを記述するＨＴＭＬファイル１６を取得して表示装置６上に存在確認ページを表示する（ステップ６１）。次に入力装置７を介して検証が指示されたとき、存在確認ページ中の文書ＵＲＬ、登録日付及びコンテンツ１７をタプルとしてハッシュを計算する（ステップ６２）。次に存在確認ページ中のハッシュＵＲＬにアクセスし、文書存在証明サーバ１に保存されたハッシュを取得する（ステップ６３）。次に取得したハッシュに文書存在証明サーバ１の電子署名が施されているか否か判定し、かつ取得したハッシュとステップ６２で計算したハッシュとを比較して両者が一致するか否か判定する（ステップ６４）。文書存在証明サーバ１の署名があり両ハッシュが一致した場合には（ステップ６４Ｙｅｓ）、処理情報の処理結果を証明成功（ＯＫ）にセットする（ステップ６５）。文書存在証明サーバ１の署名がないか両ハッシュが一致しない場合には（ステップ６４Ｎｏ）、処理結果を証明失敗（Ｆａｉｌ）にセットして（ステップ６７）、ステップ６６へ行く。最後に処理結果を表示装置６上に表示する（ステップ６６）。

【００２０】図８は、登録者端末３の表示装置６上に表示されたコンテンツ１７を示す図である。入力装置７を介して「登録」ボタンが指示されると、Ｗｅｂブラウザ１５はこのコンテンツ１７の元の文書１１の文書ＵＲＬと登録者の電子メールアドレスを文書存在証明サーバ１へ送信し、文書１１の存在証明情報を登録するよう要求する。

【００２１】図９は、登録者端末３の表示装置６上に表示された登録情報を示す図である。登録日付及び文書ＵＲＬは登録者端末３の記憶装置から取り出したもの、ハッシュへのリンクは文書存在証明サーバ１から受信したハッシュＵＲＬである。

【００２２】図１０は、登録者端末３の表示装置６に表示された存在確認ページを示す図である。コンテンツへのリンクは、コンテンツ１７の格納場所を示す情報である。入力装置７を介して「検証」ボタンが指示されると、検証処理が開始される。また閲覧者端末４の表示装置６上にも閲覧者の指示によってこの存在確認ページが表示され、同様に「検証」ボタンの指示によって検証処理が開始される。

【００２３】図１１は、閲覧者端末４の表示装置６上に表示された文書の存在を証明するメッセージを示す図である。これによって閲覧者は、指定されたコンテンツ１７の元の文書が登録日付で示される日に文書ＵＲＬで示される格納場所に存在していたことを確認することができる。入力装置７を介してコンテンツへのリンクを指示すると、Ｗｅｂブラウザ１５は記憶装置上のコンテンツ１７を表示装置６上に表示し、図８に示す表示画面となる。

【００２４】図１２は、登録者端末３及び閲覧者端末４の表示装置６に表示された参考ＵＲＬを示す図である。従来の論文において参考文献を提示するのと同様に、Ｗｅｂページに参考ＵＲＬを添付することがある。この場合、リンク先の文書に変更があった場合には参考ＵＲＬが意味をなさなくなる可能性がある。これを避けるために参考文書の複製物をコンテンツ１７として登録者端末３に保存し、このコンテンツ１７を他の閲覧者端末４に

提供することが考えられる。この場合、文書は参考ＵＲＬで示される元々存在した場所以外の場所に保存されることになる。そこで閲覧者端末４にコンテンツ１７だけでなくＨＴＭＬファイル１６、すなわち存在確認ページも提供することにすれば、閲覧者は上記の検証処理を行うことによって参考ＵＲＬで示される文書がその場所に存在していたことを確認することができる。図１２に示す例は、各参考ＵＲＬに「確認」としてコンテンツ１７へのリンクと存在確認ページのＵＲＬを付加した例である。ここでコンテンツ１７へのリンクは登録者端末３のＵＲＬに特定のコンテンツ１７の識別子を付加したものであり、存在確認ページのＵＲＬは登録者端末３のＵＲＬに特定のＨＴＭＬファイル１６の識別子を付加したものである。閲覧者端末４の入力装置７を介して「確認」が指示されたとき、Ｗｅｂブラウザ１５は、図８に示すようなコンテンツとともに図１０に示すような存在確認ページを表示装置６に表示するので、入力装置７を介して「検証」ボタンが指示されれば上記のような検証処理を実行する。

【００２５】なお上記実施形態では文書ＵＲＬ、コンテンツ及び登録日付を代表する縮小された代替情報として計算によって求められたハッシュを挙げたが、上記の目的に沿うのであればハッシュの代わりに他の方式によって生成した代替情報であってもよい。また登録ＤＢ１３に登録された各レコードに含まれる登録日付、メールアドレス及び文書ＵＲＬは、レコードを削除するときの検索キーとして利用するほかに、登録日付の古い登録者に対して電子メールによって通知するなど登録ＤＢ１３の管理のために使用される。登録ＤＢ１３の管理は本発明と直接関係しないので、ハッシュＵＲＬによって特定の登録者の特定のハッシュ１４にアクセスできるならば文書存在証明サーバ１に登録ＤＢ１３を設けなくても本発明を実施できる。

【００２６】

【発明の効果】以上説明したように本発明によれば、サーバ計算機は登録日付に指定された文書の格納場所からオリジナル文書を引き出してこれら情報の縮小された代替情報を生成して登録するので、クライアント計算機に保存された登録日付、文書の格納場所及びローカルに保存された文書の複製物から生成された代替情報とサーバに登録された代替情報とを比較することによって、ローカルに保存された文書の複製物がオリジナル文書と同じものであることを実証することができる。これによって他の閲覧者に対してローカルに保存された文書の複製物を提供するに際して、情報の信頼性や真贋の判断に関しての拠り所を与えることができる。

【図面の簡単な説明】

【図１】実施形態のシステムの構成を示す図である。

【図２】実施形態の登録ＤＢ１３のデータ構成を示す図である。

【図３】実施形態のＨＴＭＬファイル１６のデータ構成を示す図である。

【図４】実施形態の登録者端末３のＷｅｂブラウザ１５の処理の流れを示すフローチャートである。

【図５】実施形態の文書存在証明サーバ１のＷｅｂサーバプログラム１２の登録処理の流れを示すフローチャートである。

【図６】実施形態の文書存在証明サーバ１のＷｅｂサーバプログラム１２の削除処理の流れを示すフローチャートである。

【図７】実施形態の閲覧者端末４のＷｅｂブラウザ１５の検証処理の流れを示すフローチャートである。

【図８】実施形態のコンテンツ１７の表示例を示す図である。

【図９】実施形態の表示装置６上に表示される登録情報を示す図である。

【図１０】実施形態の存在確認ページの表示例を示す図である。

【図１１】実施形態の文書の存在を証明するメッセージの表示例を示す図である。

【図１２】実施形態の参考ＵＲＬと確認のためのリンクとを表示する例を示す図である。

【符号の説明】

１・・・文書存在証明サーバ、３・・・登録者端末、４・・・閲覧者端末、１２・・・Ｗｅｂサーバプログラム、１３・・・登録ＤＢ、１４・・・ハッシュ、１５・・・Ｗｅｂブラウザ、１６・・・ＨＴＭＬファイル、１７・・・コンテンツ

【図２】

図２

１３：登録ＤＢ

登録日付	メールアドレス	文書ＵＲＬ	ハッシュＵＲＬ
970707	xxx@yyy.zz	http://www.xxx.yyy/	http://hhh.yy/
・・・	・・・	・・・	・・・

【図３】

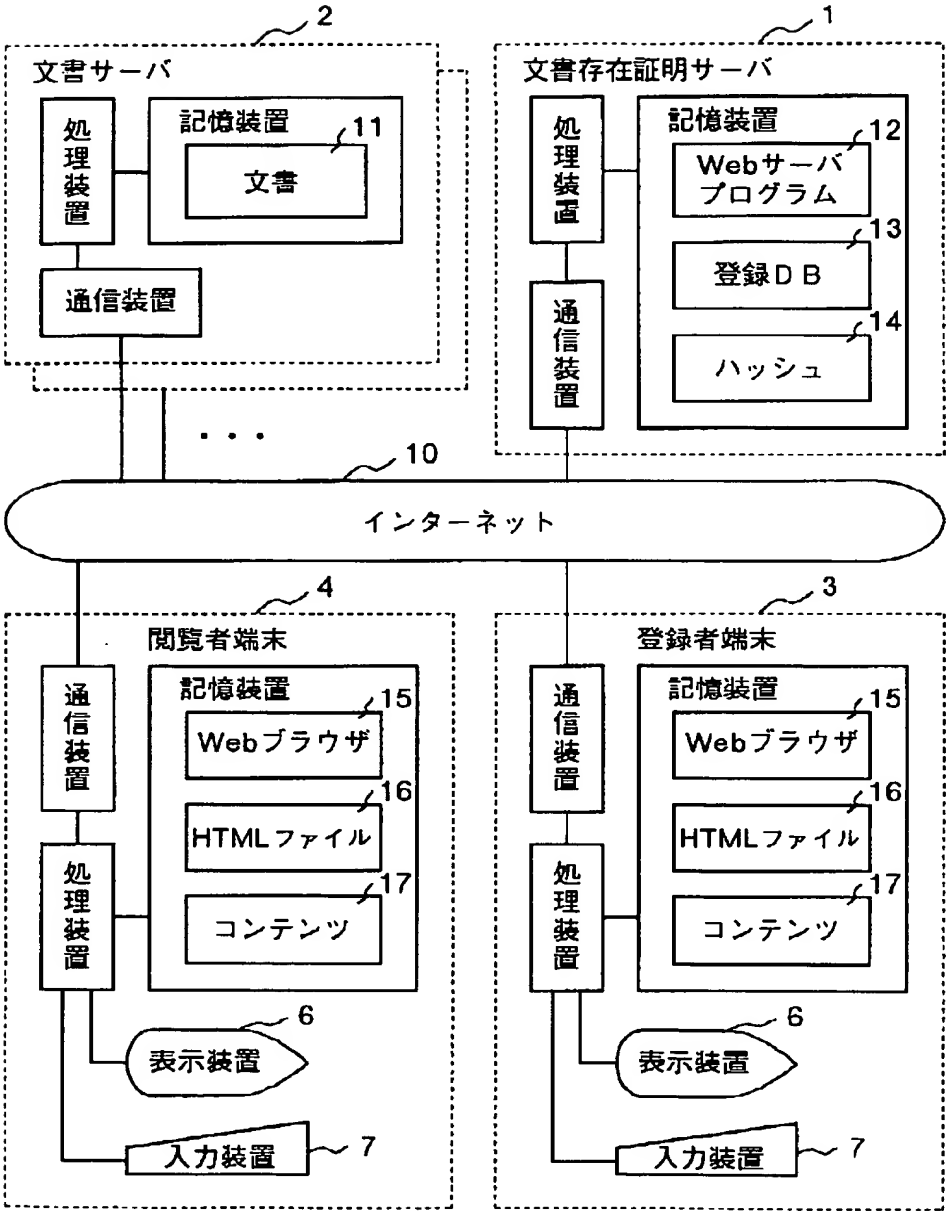
図３

１６：ＨＴＭＬファイル

・登録日付
・コンテンツの元の存在場所を示すＵＲＬ
・ローカルに保存されるコンテンツへのリンク
・存在証明サーバのハッシュＵＲＬ

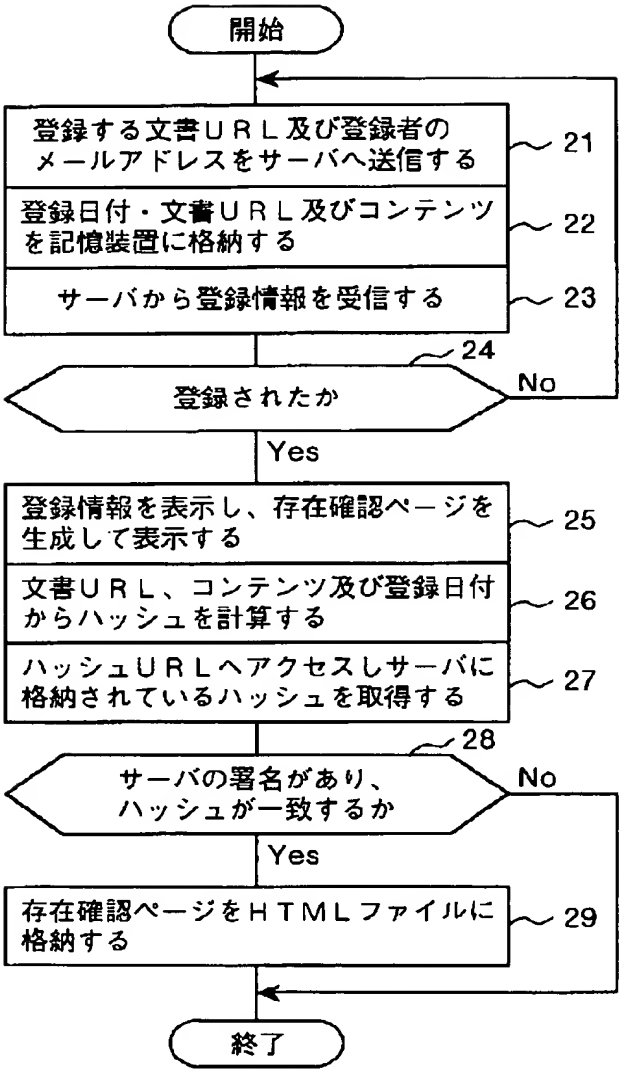
【図１】

図　1


2
文書サーバ
処理装置
記憶装置
11
文書
通信装置
1
文書存在証明サーバ
処理装置
記憶装置
12
Webサーバプログラム
13
登録ＤＢ
14
ハッシュ
通信装置
10
インターネット
4
閲覧者端末
通信装置
処理装置
記憶装置
15
Webブラウザ
16
HTMLファイル
17
コンテンツ
6
表示装置
入力装置
7
3
登録者端末
通信装置
処理装置
記憶装置
15
Webブラウザ
16
HTMLファイル
17
コンテンツ
6
表示装置
入力装置
7

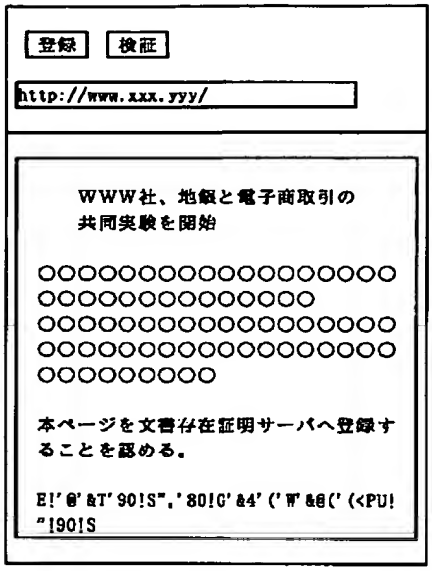
【図４】

図　4



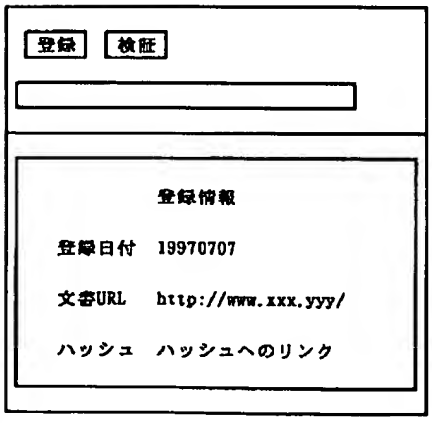
【図８】

図８



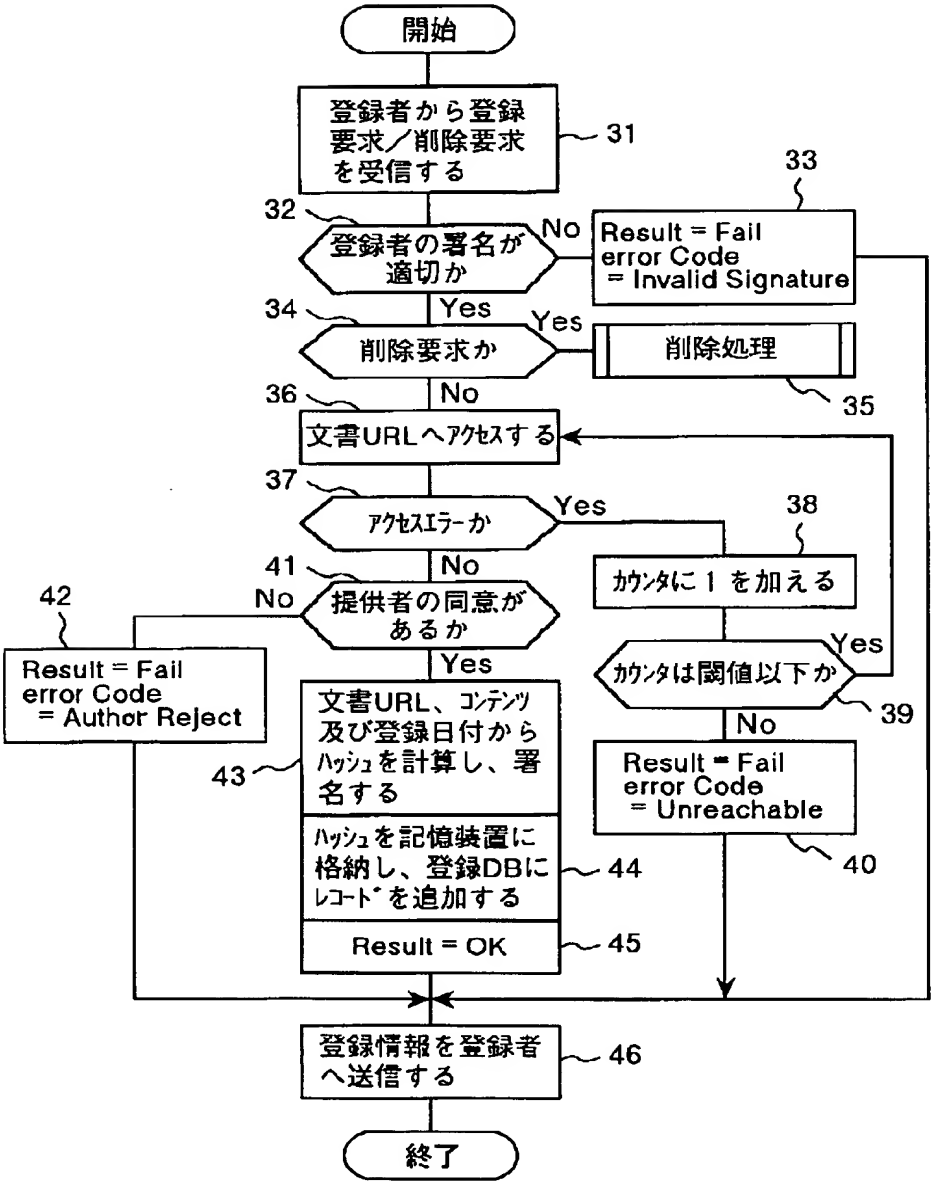
【図９】

図９



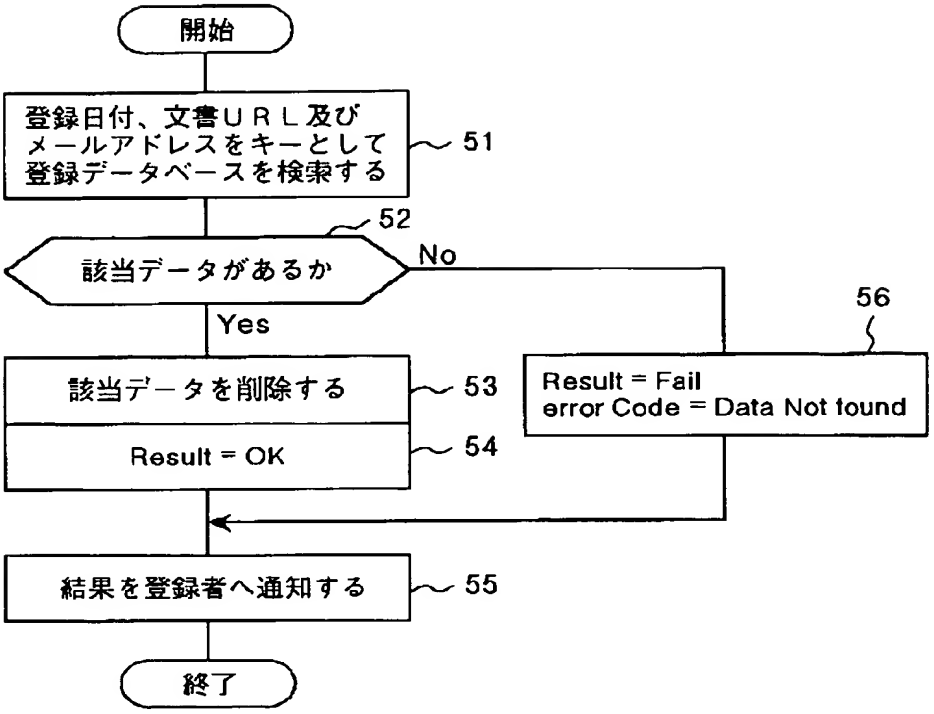
【図５】

図　5


開始
登録者から登録要求／削除要求を受信する
31
32
登録者の署名が適切か
No
33
Result = Fail
error Code
= Invalid Signature
Yes
34
削除要求か
Yes
削除処理
35
No
36
文書URLへｱｸｾｽする
37
ｱｸｾｽｴﾗｰか
Yes
38
ｶｳﾝﾀに１を加える
41
No
提供者の同意があるか
No
42
Result = Fail
error Code
= Author Reject
Yes
Yes
ｶｳﾝﾀは閾値以下か
39
No
文書URL、ｺﾝﾃﾝﾂ及び登録日付からﾊｯｼｭを計算し、署名する
43
Result = Fail
error Code
= Unreachable
40
ﾊｯｼｭを記憶装置に格納し、登録DBにﾚｺｰﾄﾞを追加する
44
Result = OK
45
登録情報を登録者へ送信する
46
終了

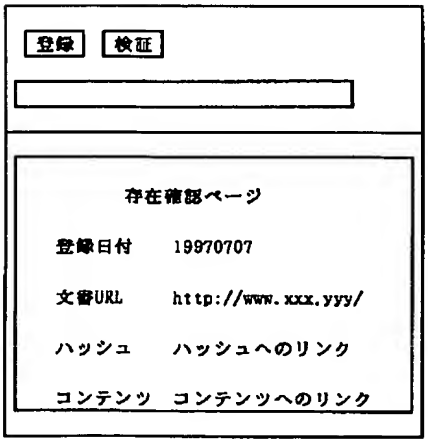
【図６】

図　6



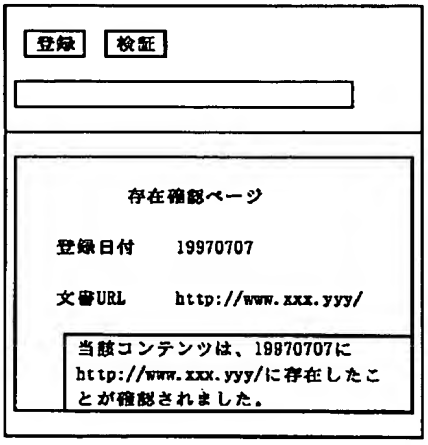
【図１０】

図１０



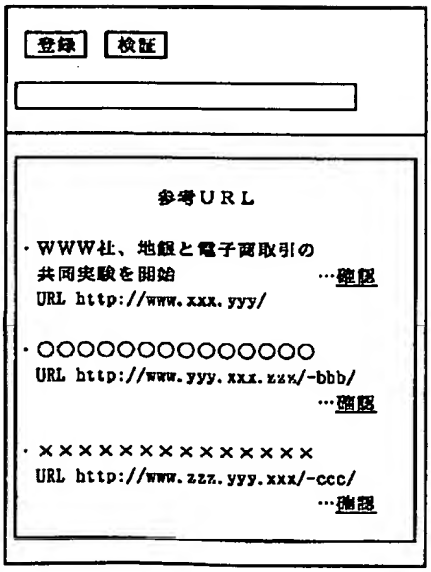
【図１１】

図１１



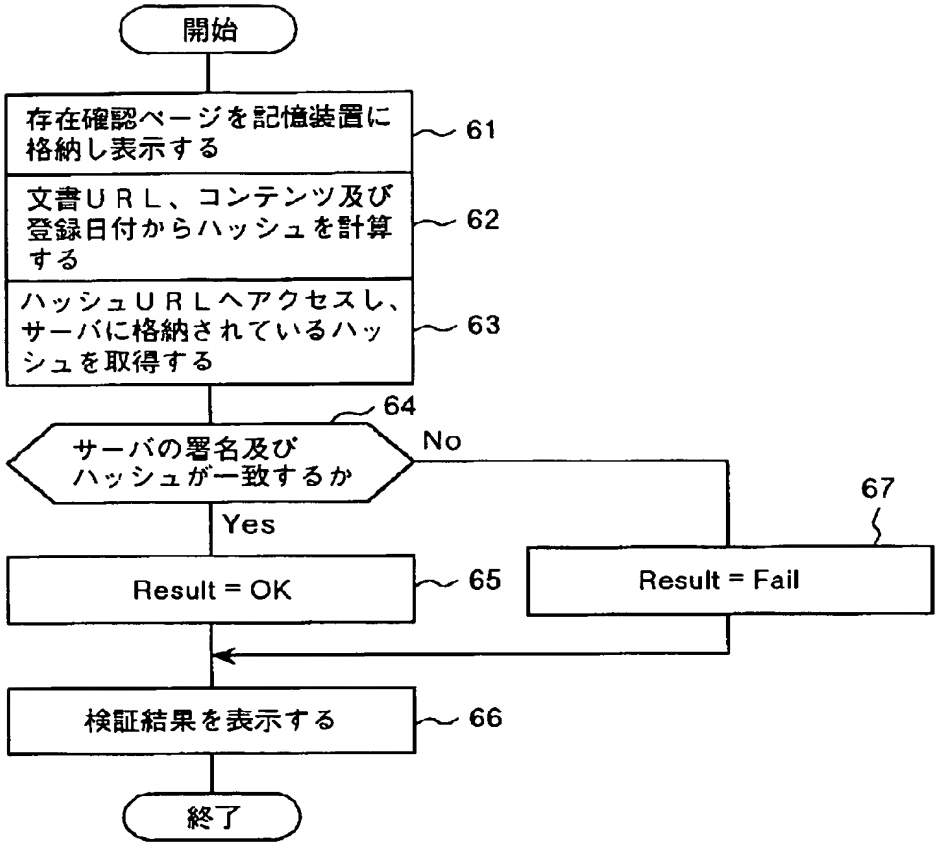
【図１２】

図１２



【図７】

図　7



フロントページの続き

(72)発明者　富山　朋哉
神奈川県横浜市都筑区加賀原二丁目２番
株式会社日立製作所ビジネスシステム開発センタ内

(72)発明者　川連　嘉晃
神奈川県横浜市都筑区加賀原二丁目２番
株式会社日立製作所ビジネスシステム開発センタ内